1. A method of creating a digital authentication pattern that contains a message, the digital authentication pattern belonging to a digital representation, and the method comprising the steps of:

selecting sets of pattern elements belonging to the digital authentication pattern to carry message elements of the message; and

for each selected set, setting the values of the pattern elements in the set to carry the message element such that the digital authentication pattern's ability to detect copying remain substantially unchanged.

2. The method set forth in claim 1 wherein:

the values are set such that the entropy of the digital authentication pattern is substantially unchanged.

3. The method set forth in claim 1, wherein:

the message elements specify values belonging to a range thereof; and

in the step of setting the values, a selected set of pattern elements is set to indicate a message element specifying one of the values of the range

4. The method set forth in claim 3 wherein:

in the step of setting the values, the selected set is set using a key.

5. The method set forth in claim 3 wherein:

the sets of pattern elements belong to categories thereof;

the category of a set of pattern elements indicates the value of a message element contained therein; and

in the step of setting the values of the pattern elements in the set, the set of pattern elements is given a category as required for the value of the message element.

6. The method set forth in claim 5, wherein:

the sets of pattern elements belong to two categories.

7. The method set forth in claim 5, wherein:

in the step of setting the values, the values of the pattern elements in the set are inverted to indicate a value belonging to a category.

8. The method set forth in claim 1, wherein:

in the step of setting the values, a value of the message is set repeatedly in the sets of pattern elements.

9. The method set forth in claim 1, wherein:

the message includes an error correction code.

10. The method set forth in claim 1, wherein:

the message is encoded using a key.

11. The method set forth in claim 1, wherein:

in the step of selecting the sets, a key is used to select the set of pattern elements that an element of the message is inserted into.

12. The method set forth in claim 1, wherein:

the pattern element is a primitive element of the digital representation to which the digital authentication pattern belongs.

13. The method set forth in claim 12, wherein:

the pattern element is a pixel.

14. The method set forth in claim 13, wherein:

the pixel is a color pixel.

15. The method set forth in claim 13, wherein:

the pixel is a gray scale pixel.

16. The method set forth in claim 13, wherein:

the pixel is a black or white pixel.

17. The method set forth in claim 12, wherein:

the digital representation is a representation of an audio signal and the pattern element is a primitive of the representation of the audio signal.

18. The method set forth in claim 12, wherein:

the digital representation is a representation of a video signal and the pattern element is a primitive of the representation of the video signal.

19. A storage device characterized in that:

the storage device contains code which, when executed by a processor, implements the method set forth in claim 1.

20. A method of reading a message whose values have been inserted into sets of pattern elements in a digital authentication pattern belonging to a digital representation,
the method comprising the steps of:

selecting sets of pattern elements belonging to the digital authentication pattern that carry message elements of the message; and

for each selected set, comparing the set with equivalent sets that have a possible value of the message element to determine the value of the message element in the selected set.

21. The method set forth in claim 20 further comprising the step of:

after the message has been read, creating an equivalent digital authentication pattern to the digital authentication pattern that contains the message, whereby the digital authentication may be compared with the equivalent digital authentication pattern to determine a copying relationship with regard to the digital representation that contains the digital authentication pattern.

22. The method set forth in claim 21 wherein:

in the step of creating the equivalent digital authentication pattern, the equivalent digital authentication pattern is created by replacing sets of pattern elements therein that do not carry message elements with equivalent sets of pattern elements that do carry message elements.

23. The method set forth in claim 20, wherein:

the message elements specify values belonging to a range thereof; and

the equivalent sets include a set for each of the values in the range thereof.

24. The method set forth in claim 23 wherein:

in the step of selecting, the selection is done using a key.

25. The method set forth in claim 23 wherein:

the sets of pattern elements belong to categories thereof;

the category of a set of pattern elements indicates the value of a message element contained therein; and

in the step of comparing, the equivalent sets include a set for each of the categories.

26. The method set forth in claim 25, wherein:

the sets of pattern elements belong to two categories.

27. The method set forth in claim 25, wherein:

in the step of comparing, a set of pattern elements whose original values have been inverted indicates a message element value corresponding to the category of the set of pattern elements.

28. The method set forth in claim 20, wherein:

a message element is repeated in the sets of pattern elements; and

the method further comprises the step of comparing sets of pattern elements containing the repeated message element to statistically determine the value of the repeated message element.

29. The method set forth in claim 20, wherein:

the message includes an error correction value; and

the method further comprises the step of using the error correction value to correct any error in the message.

30. The method set forth in claim 20, wherein:

the message is encoded using a key; and

the method includes the step of decoding the message.

31. The method set forth in claim 20, wherein:

in the step of selecting the sets, a key is used to select the sets of pattern elements that contain a message element.

32. The method set forth in claim 20, wherein:

the pattern element is a primitive element of the digital representation to which the digital authentication pattern belongs.

33. The method set forth in claim 32, wherein:

the pattern element is a pixel.

34. The method set forth in claim 33, wherein:

the pixel is a color pixel.

35. The method set forth in claim 33, wherein:

the pixel is a gray scale pixel.

36. The method set forth in claim 33, wherein:

the pixel is a black or white pixel.

37. The method set forth in claim 32, wherein:

the digital representation is a representation of an audio signal and the pattern element is a primitive of the representation of the audio signal.

38. The method set forth in claim 32, wherein:

the digital representation is a representation of a video signal and the pattern element is a primitive of the representation of the video signal.

39. A storage device characterized in that:

the storage device contains code which, when executed by a processor, implements the method set forth in claim 1.

40. A digital authentication pattern that contains a message,

the digital authentication pattern comprising:

a plurality of sets of pattern elements, the plurality of sets of pattern elements including sets thereof that carry message elements belonging to the message; and

in a set that carries message elements, setting the values of the pattern elements in the set to carry the message element such that the digital authentication pattern's ability to detect copying remain substantially unchanged.

41. The method set forth in claim 40 wherein:

the values are set such that the entropy of the digital authentication pattern is substantially unchanged.

42. A method of determining whether an analog form that includes a copy detection pattern is an original analog form,

the method comprising the steps of:

scanning the copy detection pattern to produce a digital representation thereof; and

using one or more global properties of the digital representation of the scanned copy detection pattern to make at least a preliminary determination of whether the analog form is an original analog form, the preliminary determination being made without reference to a digital representation of the original of the analog form's copy detection pattern.

43. A method of determining a copying relationship between digital representations, each of the digital representations including a portion that is sensitive to alterations produced by a copying process and the method comprising the steps of:

modifying a portion to make the portion more comparable with the other portion by taking the alterations into account; and

comparing the portions to determine the copying relationship.

44. A visual authentication pattern for a document, the visual authentication pattern having high entropy and being sensitive to the effects of print and scan operations and being characterized in that:

the visual authentication pattern is subdivided into units which are distributed across the document.

45. The visual authentication pattern set forth in claim 44 further characterized in that:

the distribution of the units across the document is determined using a key.

46. The visual authentication pattern set forth in claim 45 further characterized in that:

when the visual authentication pattern is analyzed, the key is used to locate the units.

47. The visual authentication pattern set forth in claim 46 further characterized in that:

the key is a secret key.

48. The visual authentication pattern set forth in claim 44 further characterized in that:

certain of the units have specific properties whereby the units may be located; and

when the visual authentication pattern is analyzed, the certain units are used to locate other units.

49. The visual authentication pattern set forth in claim 44 further characterized in that:

a unit contains one or more pixels; and

the values of the pixels in the unit are adjusted to make the unit less perceptible at the unit's location in the document.

50. The visual authentication pattern set forth in claim 49 further characterized in that:

the density with which the units are distributed across an area of the document is adjusted to make the units less perceptible.

51. The visual authentication pattern set forth in claim 44 further characterized in that:

the distributed units form a visual pattern in the document.

52. A method of locating a visual authentication pattern in a digital representation of a document,

the method comprising the steps of:

determining the entropy of an area of the digital representation of the document; and

comparing the determined entropy with an entropy for the visual authentication pattern to determine whether the area belongs to the visual authentication pattern.

53. A digital representation of an analog signal,

the digital representation being characterized in that:

the digital representation includes a representation of a copy detection signal that is sensitive to transformations produced by digital-to-analog and analog-to-digital conversions, whereby the representation of the copy detection signal may be used to determine whether another digital representation of the analog signal was made by digitizing an analog signal produced from the digital representation.

54. A digital representation characterized in that:

the digital representation includes a first portion wherein the data has error correction and a second portion wherein the data has no error correction and the data is sensitive to alterations produced by the process of making a digital copy of the digital representation, whereby the second portion may be used to determine a copy relationship between the digital representation and another digital representation.